Getting Started Guide

Cisco Aironet 3500 Series Lightweight Access Point

1 About this Guide
2 Safety Instructions
3 Unpacking
4 Overview
5 Configuring the Access Point
6 Mounting the Access Point
7 Deploying the Access Point on the Wireless Network
8 Troubleshooting
9 Declarations of Conformity and Regulatory Information
10 Configuring DHCP Option 43 and DHCP Option 60
11 Access Point Specifications

1 About this Guide

This Guide provides instructions on how to install and configure your Cisco Aironet 3500 Series Access Point. This guide also provides mounting instructions and limited troubleshooting procedures.

2 Safety Instructions

Translated versions of the following safety warnings are provided in the translated safety warnings document that is shipped with your access point. The translated warnings are also in the *Translated Safety Warnings for Cisco Aironet Access Points*, which is available on your documentation CD and Cisco.com.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

Warning **This product must be connected to a Power-over-Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.** Statement 353

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20A.** Statement 1005

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.** Statement 332

Caution The fasteners you use to mount an access point on a ceiling must be capable of maintaining a minimum pullout force of 20 lbs (9 kg) and must use all 4 indented holes on the mounting bracket.

Caution This product and all interconnected equipment must be installed indoors within the same building, including the associated LAN connections as defined by Environment A of the IEEE 802.af Standard.

Note The access point is suitable for use in environmental air space in accordance with section 300.22.C of the National Electrical Code and sections 2-128, 12-010(3), and 12-100 of the Canadian Electrical Code, Part 1, C22.1. You should not install the power supply or power injector in air handling spaces.

Note Use only with listed ITE equipment.

3 Unpacking

Follow these steps:

Step 1 Unpack and remove the access point and the accessory kit from the shipping box.

Step 2 Return any packing material to the shipping container and save it for future use.

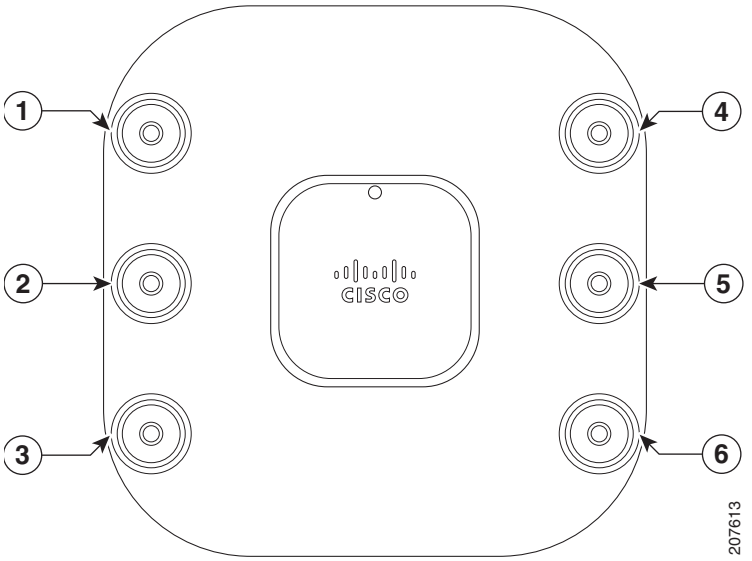
Step 3 Verify that you have received the items listed below. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

- 3500 series access point
- Mounting bracket (selected when you ordered the access point)
- Adjustable ceiling-rail clip (selected when you ordered the access point)

4 Overview

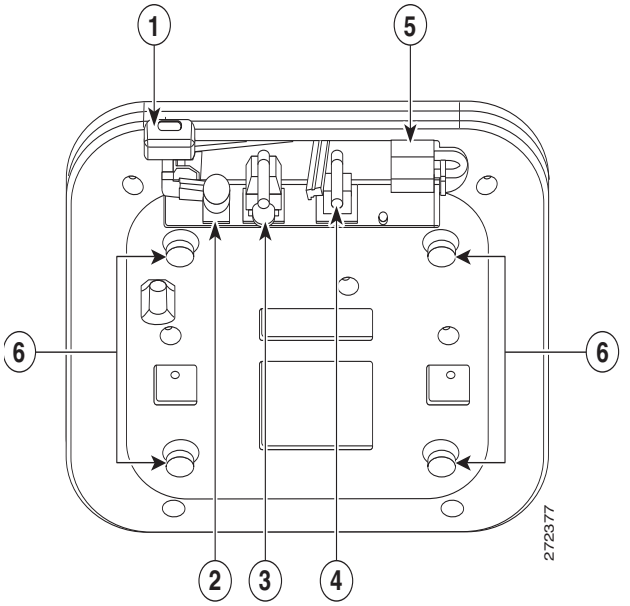
The following illustrations show the access point connections and features. The 3500e access point has external antenna connectors; the 3500i access point has integrated antennas and does not have external connectors.

Figure 1 Access Point Ports and Connections (top)



1	2.4-GHz antenna connector B (labelled with black text)	**4**	5-GHz antenna connector A (labelled with blue text)
2	2.4-GHz antenna connector C (labelled with black text)	**5**	5-GHz antenna connector C (labelled with blue text)
3	2.4-GHz antenna connector A (labelled with black text)	**6**	5-GHz antenna connector B (labelled with blue text)

Figure 2 Access Point Ports and Connections (bottom)



1	Kensington lock slot	**4**	Console port
2	Power connection	**5**	Security padlock and hasp (padlock not included)
3	Ethernet port	**6**	Mounting bracket pins (feet for desk or table-top mount)

5 Configuring the Access Point

This section describes how to connect the access point to a wireless LAN controller. Because the configuration process takes place on the controller, see the *Cisco Wireless LAN Controller Configuration Guide* for additional information. This guide is available on Cisco.com.

The Controller Discovery Process

The 3500 series access point uses the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, interoperable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Note For additional information about the discovery process and CAPWAP, see the *Cisco Wireless LAN Controller Software Configuration Guide*. This document is available on Cisco.com.

Note CAPWAP support is provided in controller software release 5.2 or later. However, your controller must be running release 7.0 or later to support 3500 series access points.

Note You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

Note Make sure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The 3500 series access point supports these controller discovery processes:

- **Layer 3 CAPWAP discovery**—Can occur on different subnets than the access point and uses IP addresses and UDP packets rather than MAC addresses used by Layer 2 discovery.
- **Over-the-air provisioning (OTAP)**—This feature is supported by Cisco 4400 series controllers. If this feature is enabled on the controller, all joined access points transmit wireless CAPWAP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.

  Additional information about OTAP is available on Cisco.com at the following link:

  http://www.ciscosystems.com/en/US/products/ps6366/products_tech_note09186a008093d74a.shtml
- **Locally stored controller IP address discovery**—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called *priming the access point*. For more information about priming, see the "Performing a Pre-Installation Configuration" section on page 9.
- **DHCP server discovery**—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43 and DHCP Option 60" section on page 30.
- **DNS discovery**—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Preparing the Access Point

Before you mount and deploy your access point, we recommend that you perform a site survey (or use the site planning tool) to determine the best location to install your access point.

You should have the following information about your wireless network available:

- Access point locations.
- Access point mounting options: below a suspended ceiling, on a flat horizontal surface, or on a desktop.

Note You can mount the access point above a suspended ceiling but you must purchase additional mounting hardware: See "Mounting the Access Point" section on page 13 for additional information.

- Access point power options: power supplied by the recommended external power supply (Cisco AIR-PWR-B), a DC power supply, PoE from a network device, or a PoE power injector/hub (usually located in a wiring closet).

Note Access points mounted in a building's environmental airspace must be powered using PoE to comply with safety regulations.

Cisco recommends that you make a site map showing access point locations so that you can record the device MAC addresses from each location and return them to the person who is planning or managing your wireless network.

Installation Summary

Installing the access point involves these operations:

- Performing a pre-installation configuration (optional)
- Mounting the access point
- Grounding the access point
- Deploying the access point on the wireless network

Performing a Pre-Installation Configuration

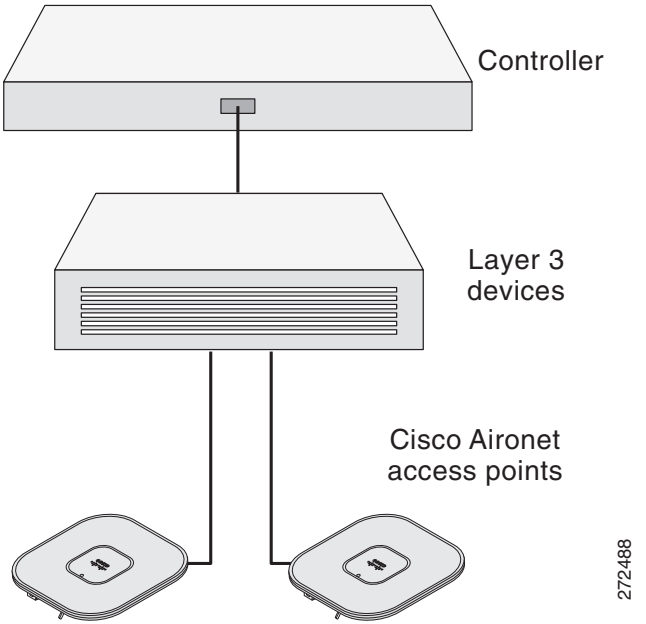
The following procedures ensure that your access point installation and initial operation go as expected. A pre-installation configuration is also known as *priming the access point*. This procedure is optional.

Note Performing a pre-installation configuration is an optional procedure. If your network controller is properly configured, you can install your access point in its final location and connect it to the network from there. See the "Deploying the Access Point on the Wireless Network" section on page 13 for details.

Pre-Installation Configuration Setup

Figure 3 shows the pre-installation configuration setup.

Figure 3 Pre-Installation Configuration Setup



Follow these steps to perform the pre-installation configuration.

Step 1 Make sure that the Cisco wireless LAN controller DS port is connected to the network. Use the CLI, web-browser interface, or Cisco WCS procedures as described in the appropriate Cisco wireless LAN controller guide.

- **a.** Make sure that access points have Layer 3 connectivity to the Cisco wireless LAN controller Management and AP-Manager Interface.
- **b.** Configure the switch to which your access point is to attach. See the *Cisco Unified Wireless Network WLAN Controller Guide: Cisco 440x Series WLAN Controllers* for additional information.
- **c.** Set the Cisco wireless LAN controller as the master so that new access points always join with it.
- **d.** Make sure DHCP is enabled on the network. The access point must receive its IP address through DHCP.

e. CAPWAP UDP ports must not be blocked in the network.

f. The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the "Using DHCP Option 43" section on page 14 for more information.

Step 2 Apply power to the access point:

a. The access point is 802.3af (15.4 W) compliant and can be powered by any of the following 802.3af compliant devices:

- 2106 controller
- WS-C3550, WS-C3560, and WS-C3750 switches
- C1880 switch
- 2600, 2610, 2611, 2621, 2650, and 2651 multiservice platforms
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, and 2691 multiservice platforms
- 2811, 2821, and 2851 integrated services routers
- 3620, 3631-telco, 3640, and 3660 multiservice platforms
- 3725 and 3745 multiservice access routers
- 3825 and 3845 integrated services routers

The recommended external power supply for the access point is the Cisco AIR-PWR-B power supply. The access point can also be powered by the following optional external power sources:

- 1250 series access point power injector (AIR-PWRINJ4)
- Any 802.3af compliant power injector

Note The 3500 series access point requires a Gigibit Ethernet link to prevent the Ethernet port from becoming a bottleneck for traffic because wireless traffic speeds exceed transmit speeds of a 10/100 Ethernet port.

b. As the access point attempts to connect to the controller, the LEDs cycle through a green, red, and amber sequence, which can take up to 5 minutes.

Note If the access point remains in this mode for more than five minutes, the access point is unable to find the Master Cisco wireless LAN controller. Check the connection between the access point and the Cisco wireless LAN controller and be sure that they are on the same subnet.

c. If the access point shuts down, check the power source.

d. After the access point finds the Cisco wireless LAN controller, it attempts to download the new operating system code if the access point code version differs from the Cisco wireless LAN controller code version. While this is happening, the Status LED blinks dark blue.

e. If the operating system download is successful, the access point reboots.

Step 3 Configure the access point if required. Use the controller CLI, controller GUI, or Cisco WCS to customize the access-point-specific 802.11n network settings.

Step 4 If the pre-installation configuration is successful, the Status LED is green indicating normal operation. Disconnect the access point and mount it at the location at which you intend to deploy it on the wireless network.

Step 5 If your access point does not indicate normal operation, turn it off and repeat the pre-installation configuration.

Note When you are installing a Layer 3 access point on a different subnet than the Cisco wireless LAN controller, be sure that a DHCP server is reachable from the subnet on which you will be installing the access point, and that the subnet has a route back to the Cisco wireless LAN controller. Also be sure that the route back to the Cisco wireless LAN controller has destination UDP ports 5246 and 5247 open for CAPWAP communications. Ensure that the route back to the primary, secondary, and tertiary wireless LAN controller allows IP packet fragments. Finally, be sure that if address translation is used, that the access point and the Cisco wireless LAN controller have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)

6 Mounting the Access Point

Cisco Aironet 3500, 1260, 1140, 1130, and 1040 series access points can be mounted in several configurations, including on a suspended ceiling, on a hard ceiling or wall, on an elecrtical or network box, and above a suspended ceiling. Click this URL to browse to complete access point mounting instructions:

http://www.cisco.com/en/US/docs/wireless/access_point/mounting/guide/apmount.html

7 Deploying the Access Point on the Wireless Network

After you have mounted the access point, follow these steps to deploy it on the wireless network.

Step 1 Connect and power up the access point.

Step 2 Observe the access point LED.

- **a.** When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks sequentially green, red, and off. When the access point has joined a controller, the LED is green if no clients are associated or blue if one or more clients are associated.
- **b.** If the LED is not on, the access point is most likely not receiving power.
- **c.** If the LED blinks sequentially for more than 5 minutes, the access point is unable to find its primary, secondary, and tertiary Cisco wireless LAN controller. Check the connection between the access point and the Cisco wireless LAN controller, and be sure the access point and the Cisco wireless LAN controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco wireless LAN controller. Also, if the access point is not on the same subnet as the Cisco wireless LAN controller, be sure that there is a properly configured DHCP server on the same subnet as the access point. See the "Configuring DHCP Option 43 and DHCP Option 60" section on page 30 for additional information.

Step 3 Reconfigure the Cisco wireless LAN controller so that it is not the Master.

Note A Master Cisco wireless LAN controller should be used only for configuring access points and not in a working network.

8 Troubleshooting

If you experience difficulty getting your access point installed and running, look for a solution to your problem in this guide or in additional access point documentation. These, and other documents, are available on Cisco.com.

Guidelines for Using Cisco Aironet Lightweight Access Points

Keep these guidelines in mind when you use 3500 series lightweight access points:

- The access point can only communicate with Cisco wireless LAN controllers, such as 2100, 4400, and 5500 series controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

Using DHCP Option 43

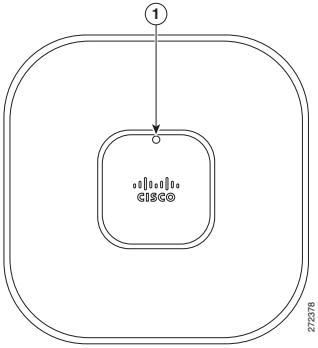
You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling them to find and join a controller. For additional information, refer to the "Configuring DHCP Option 43 and DHCP Option 60" section on page 30.

Checking the Access Point LED

Figure 4 shows the location of the access point Status LED.

Note Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect.

Figure 4 Access Point LED Location



1	Status LED	

Table 1 shows the access point Status LED indications for various conditions.

Table 1 LED Status Indications

Message Type	**Status LED**	**Message Meaning**
Boot loader status sequence	Blinking green	DRAM memory test in progress
		DRAM memory test OK
		Board initialization in progress
		Initializing FLASH file system
		FLASH memory test OK
		Initializing Ethernet
		Ethernet OK
		Starting Cisco IOS
		Initialization successful
Association status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association

Table 1 LED Status Indications (continued)

Message Type	Status LED	Message Meaning
Operating status	Blinking blue	Software upgrade in progress
	Cycling through green, red, and off	Discovery/join process in progress
	Rapidly cycling through blue, green, and red	Access point location command invoked
	Blinking red	Ethernet link not operational
Boot loader warnings	Blinking blue	Configuration recovery in progress (MODE button pushed for 2 to 3 seconds)
	Red	Ethernet failure or image recovery (MODE button pushed for 20 to 30 seconds)
	Blinking green	Image recovery in progress (MODE button released)
Boot loader errors	Red	DRAM memory test failure
	Blinking red and blue	FLASH file system failure
	Blinking red and off	Environment variable failure
		Bad MAC address
		Ethernet failure during image recovery
		Boot environment failure
		No Cisco image file
		Boot failure
Cisco IOS errors	Red	Software failure; try disconnecting and reconnecting unit power
	Cycling through blue, green, red, and off	General warning; insufficient inline power

Troubleshooting the Access Point Join Process

Access points can fail to join a controller for many reasons: a RADIUS authorization is pending; self-signed certificates are not enabled on the controller; the access point's and controller's regulatory domains don't match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point. Therefore, it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining problems without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to it and maintains information for any access points that have successfully joined it.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

You can view join-related information for the following numbers of access points:

- Up to 300 access points for 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch
- Up to three times the maximum number of access points supported by the platform for the 2100 series controllers and the Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default when any of the following conditions are met:

- An access point running software release 5.2 or later has been newly deployed.
- An existing access point running software release 5.2 or later has been reset after clearing the configuration.

If any of these conditions are met and the access point has not yet joined a controller, you can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global syslog_server_IP_address** command. In this case, the controller sends the new global syslog server IP address to the access point.

- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific Cisco_AP syslog_server_IP_address** command. In this case, the controller sends the new specific syslog server IP address to the access point.
- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points and view the access point join information only from the controller CLI.

A detailed explanation of the join process is on Cisco.com at the following URL:

http://www.Cisco.com/en/US/products/ps6366/products_tech_note09186a00808f8599.shtml

9 Declarations of Conformity and Regulatory Information

This section provides declarations of conformity and regulatory information for the Cisco Aironet 3500 Series Access Point.

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Models	Certification Numbers
AIR-CAP3501E-A-K9 AIR-CAP3501I-A-K9	LDK102072
AIR-CAP3502I-A-K9 AIR-CAP3502E-A-K9	LDK102073

Manufacturer:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This device operates in the 5150-5250MHz and 5470-5725MHz bands and is therefore restricted to indoor operation only per FCC guidance.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

⚠

Caution Within the 5.15 to 5.25 GHz and 5.47-5.725 GHz bands, this device is restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite System (MSS) operations.

VCCI Statement for Japan

Warning

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio Interference. Install and use the equipment according to the instruction manual.

VCCI-B

警告 この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

ＶＣＣＩ－Ｂ

Guidelines for Operating Cisco Aironet Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet access points in Japan. These guidelines are provided in both Japanese and English.

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。

2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。

3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-6434-6500

208697

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

   Contact Number: 03-6434-6500

Statement 371—Power Cable and AC Adapter

接続ケーブル、電源コード、AC アダプタ、バッテリーなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となります。また、電気用品安全法により、当該法の認定（PSE とコードに表記）でなく UL 認定（UL または CSA マークがコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

Industry Canada

Canadian Compliance Statement

AIR-CAP3501E-A-K9 AIR-CAP3501I-A-K9	2461B-102072
AIR-CAP3502E-A-K9 AIR-CAP3502I-A-K9	2461B-102073

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco Aironet Access Points are certified to the requirements of RSS-210. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

This device has been designed to operate with antennas having a maximum gain of 6 dBi. Antennas having a gain greater than 6 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Models:

AIR-CAP3501E-E-K9
AIR-CAP3502E-E-K9

AIR-CAP3501I-E-K9
AIR-CAP3502I-E-K9

Declaration of Conformity with regard to the R&TTE Directive 1999/5/EC & Medical Directive 93/42/EEC

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviešu [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]	Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

142730

The following standards were applied:

EMC—EN 301.489-1 v1.4.1; EN 301.489-17 v1.2.1

Health & Safety—EN60950-1: 2001; EN 50385: 2002

Radio—EN 300 328 v 1.7.1; EN 301.893 v 1.5.1

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

This device also conforms to the EMC requirements of the Medical Devices Directive 93/42/EEC.

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

The product carries the CE Mark:

Declaration of Conformity for RF Exposure

United States

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on ANSI C 95.1 and FCC OET Bulletin 65C rev 01.01. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

Canada

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on RSS-102 Rev 2. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

European Union

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

Australia

This system has been evaluated for RF exposure for Humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operating Cisco Aironet access points in Taiwan. The rules for all access points are provided in both Chinese and English.

Chinese Translation

低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Chinese Translation

低功率射頻電機技術規範

4.7 無線資訊傳輸設備

4.7.5 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

4.7.6 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

202591

English Translation

Low-power Radio-frequency Devices Technical Specifications

4.7 Unlicensed National Information Infrastructure

4.7.5 Within the 5.25-5.35 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

4.7.6 The U-NII devices shall accept any interference from legal communications and shall not interfere the legal communications. If interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

4.7.7 Manufacturers of U-NII devices are responsible for ensuring frequency stability such that an emission is maintained within the band of operation under all conditions of normal operation as specified in the user manual.

Operation of Cisco Aironet Access Points in Brazil

This section contains special information for operation of Cisco Aironet access points in Brazil.

Access Point Models

AIR-CAP3501E-A-K9
AIR-CAP3501I-A-K9
AIR-CAP3502E-T-K9
AIR-CAP3502I-T-K9

Regulatory Information

Figure 5 contains Brazil regulatory information for the access point models identified in the previous section.

Figure 5 Brazil Regulatory Information

Portuguese Translation

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

English Translation

This equipment operates on a secondary basis and consequently must accept harmful interference, including interference from stations of the same kind. This equipment may not cause harmful interference to systems operating on a primary basis.

Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following location: http://www.ciscofax.com

10 Configuring DHCP Option 43 and DHCP Option 60

This section contains a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Aironet lightweight access points. For other DHCP server implementations, consult product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

The 3500 series access point uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI string for the 3500 series access point is:

Cisco AP c3500

Note If your access point was ordered with the Service Provider Option (AIR-OPT60-DHCP) selected in the ordering tool, the VCI string for the access point contains *ServiceProvider*. For example, an AP3500 with this option will return this VCI string:
Cisco AP c3500-ServiceProvider

The format of the TLV block is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
<pool name> is the name of the DHCP pool, such as AP3500
<IP Network> is the network IP address where the controller resides, such as
10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "VCI string"

For the VCI string, "Cisco AP c3500". The quotation marks must be included.
```

Step 4 Add the option 43 line using the following syntax:

option 43 hex *<hex string>*

The *hex string* is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.

11 Access Point Specifications

Table 2 lists the technical specifications for 3500 series access points.

Table 2 Access Point Specifications

Category	Specification
Dimensions (LxWxD)	8.68 x 8.68 x 1.84 in. (22.04 x 22.04 x 4.67 cm)
Weight	1.9 lbs (0.86 kg)
Operating temperatures	AP3500e: -4 to 131 degrees F (-20 to 55 degrees C) AP3500i: 32 to 104 degrees F (0 to 40 degrees C)
Storage temperature	–22 to 185 degrees F (–30 to 85 degrees C)
Humidity	10% to 90% (noncondensing)
Antennas	AP3500i: Integrated; AP3500e: External
Compliance	The 3500 series access point complies with UL 2043 for products installed in a building's environmental air handling spaces, such as above suspended ceilings.

Table 2 Access Point Specifications (continued)

Category	Specification
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 IEC 60950-1 with all national deviations EN 60950-1 UL 2043
EMI and Susceptibility	FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) EN 301.489 EN 55022 Class B, 2000 version EN 55024 VCCI Class B
Radio	FCC Part 15.247, 15.407 Canada RSS-210 Japan Telec 33, 66, T71 EN 330.328, EN 301.893 FCC Bulletin OET-65C Industry Canada RSS-102
Maximum power and channel settings	Maximum power and the channels allowed in your regulatory domain, refer to *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points*. This document is available on Cisco.com.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 800 020 0791
Fax: 31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2010 Cisco Systems, Inc. All rights reserved.

OL-16415-01